AMENDED IN SENATE JANUARY 17, 2008

AMENDED IN SENATE JANUARY 7, 2008

SENATE BILL No. 364

Introduced by Senator Simitian

February 20, 2007

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 364, as amended, Simitian. Personal information: privacy.

Existing law requires any agency, and any person or business conducting business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the system or data, as defined, following discovery or notification of the security breach, to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

This bill would require the agency, person, or business, in addition to the duties specified above, to electronically report the breach to the Office of Information Security and Privacy Protection, as specified. The bill would require the office to establish a Web site where an agency, person, or business shall submit electronically to the office security breach notifications meeting specified requirements and sent to California residents; the bill would require the office to make those notifications publicly available. The bill would require the office to annually report a summary of the information collected and made available via the Web site to the Legislature.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 1798.29 of the Civil Code is amended to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, and shall submit electronically any security breach notification sent to California residents pursuant to this section to the Office of Information Security and Privacy Protection in accordance with this section. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) The Office of Information Security and Privacy Protection shall establish a Web site where agencies subject to this section shall submit electronically security breach notifications sent to California residents, and shall make these notifications publicly available online.

(e) A security breach notification shall meet all of the following requirements:

(1) The security breach notification shall be provided by ~~the~~ one of *the* following means:

(A) Written notice.

(B) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(C) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed ~~one hundred thousand dollars ($100,000)~~ *two hundred fifty thousand dollars ($250,000)*, or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of any of the following:

(i) E-mail notice when the agency has an e-mail address for the subject persons.

(ii) Conspicuous posting of the notice on the agency's Web site, if the agency maintains one.

(iii) Notification to major statewide media and electronic submission of a copy of the security breach notification form or forms to the Office of Information Security and Privacy Protection in accordance with subdivision (d).

(2) The security breach notification shall be written in plain ~~English~~ *language*.

(3) The security breach notification shall include, at a minimum, the following information:

(A) The toll-free telephone numbers and addresses of the major credit reporting agencies.

(B) The name and contact information of the reporting agency.

(C) A list of the types of information, such as name or social security number, that *were or* may have been the subject of a breach.

(D) The date of a breach, if known, and the date of discovery of a breach, if known.

(E) The date of the notification, and whether the notification was delayed pursuant to subdivision (c).

(F) A general description of the breach incident.

(G) The estimated number of persons affected by the breach.

(H) Whether substitute notice was used.

(4) The Office of Information Security and Privacy Protection shall annually report a summary of the information collected and made available via the Web site to the Legislature.

(f) For purposes of this section, the following terms have the following meanings:

(1) "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(2) (A) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(i) Social security number.

(ii) Driver's license number or California Identification Card number.

(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information.

(B) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(3) "Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(4) "Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(g) Notwithstanding *paragraphs (1) and (4) of* subdivision (e), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part *and paragraphs (2) and (3) of subdivision (e)* shall be deemed to be in compliance with the notification

requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 2. Section 1798.82 of the Civil Code is amended to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, and shall submit electronically any security breach notification sent to California residents pursuant to this section to the Office of Information Security and Privacy Protection in accordance with this section. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) The Office of Information Security and Privacy Protection shall establish a Web site where any person or business subject to this section shall submit electronically security breach notifications sent to California residents, and shall make those notifications publicly available online.

(e) A security breach notification shall meet all of the following requirements:

(1) The security breach notification shall be provided by ~~the~~ one of *the* following means:

(A) Written notice.

(B) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(C) Substitute notice, if the person or business subject to this section demonstrates that the cost of providing notice would exceed ~~one hundred thousand dollars ($100,000)~~ *two hundred fifty thousand dollars ($250,000)*, or that the affected class of subject persons to be notified exceeds 500,000, or that the person or business subject to this section does not have sufficient contact information. Substitute notice shall consist of any of the following:

(i) E-mail notice when the person or business subject to this section has an e-mail address for the subject persons.

(ii) Conspicuous posting of the notice on the person's or business' Web site, if the person or business subject to this section maintains one.

(iii) Notification to major statewide media and electronic submission of a copy of the security breach notification to the Office of Information Security and Privacy Protection in accordance with subdivision (d).

(2) The security breach notification shall be written in plain ~~English~~ *language*.

(3) The security breach notification shall include, at a minimum, the following information:

(A) The toll-free telephone numbers and addresses of the major credit reporting agencies.

(B) The name and contact information of the reporting person or business subject to this section.

(C) A list of the types of information, such as name or social security number, that *were or* may have been the subject of a breach.

(D) The date of a breach, if known, and the date of discovery of a breach, if known.

(E) The date of the notification, and whether the notification was delayed pursuant to subdivision (c).

(F) A general description of the breach incident.

(G) The estimated number of persons affected by the breach.

(H) Whether substitute notice was used.

(4) The Office of Information Security and Privacy Protection shall annually report a summary of the information collected and made available via the Web site to the Legislature.

(f) For purposes of this section, the following terms have the following meanings:

(1) "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(2) (A) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(i) Social security number.

(ii) Driver's license number or California Identification Card number.

(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information.

(B) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(3) "Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(4) "Health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(g) Notwithstanding *paragraphs (1) and (4) of* subdivision (e), a person or business subject to this section that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part *and paragraphs (2) and (3) of subdivision (e)*, shall be deemed to be in compliance

with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

O